Examples
Group, polynomial, and Hamming codes

27^{th} January, 2006

1. Construct a Hamming code with three check digits.

Solution. Choose $r = 3$. Then the code words will have $n = 2^r - 1 = 2^3 = 7$ digits, and the message words $m = 2^r - r - 1 = 2^3 - 3 - 1 = 4$ digits. In each code word there are r check digits. The redundancy of the code is r. The check digits are formed as follows.

$$\overbrace{\begin{array}{cccccc} b_1 & b_2 & b_3 & b_4 & \cdots & b_n \\ \downarrow & \downarrow & & \downarrow & \downarrow & \\ b_{2^0} & b_{2^1} & & b_{2^2} & b_{2^{r-1}} & \end{array}}^{b}$$

$$\underbrace{b_{2^0} \quad b_{2^1} \quad b_{2^2} \quad b_{2^{r-1}}}_{r \text{ check digits}}$$

The rest of the code word are the $2^r - r - 1$ message digits in their usual order. Then for our present problem.

$$\begin{array}{lccccccc} \text{check digits} & b_1 & b_2 & & b_4 & & & \\ & \uparrow & \uparrow & & \uparrow & & & \\ \text{code word} & b_1 & b_2 & b_3 & b_4 & b_5 & b_6 & b_7 \\ & & & \downarrow & & \downarrow & \downarrow & \downarrow \\ \text{message word} & & & a_1 & & a_2 & a_3 & a_4 \end{array}$$

Next, form a $(2^r - 1) \times r$ matrix M, where the i^{th} row is the binary representation of the number i.

$$M = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

Then form the matrix equation $\mathbf{b}M = 0$ which gives r linear equations in the r unknowns $b_1, b_2, \ldots, b_{2^{r-1}}$.

$$\begin{pmatrix} b_1 & b_2 & b_3 & b_4 & b_5 & b_6 & b_7 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} = \mathbf{0}$$

This gives us

$$b_4 + b_5 + b_6 + b_7 = 0$$
$$b_2 + b_3 + b_6 + b_7 = 0$$
$$b_1 + b_3 + b_5 + b_7 = 0$$

To encode a message word, we place the message in its proper positions, then find b_{2^i}, where $0 \leq i \leq r - 1$. For example, the message $a_1\, a_2\, a_3\, a_4 = 1001$ yields

$$\begin{pmatrix} b_1 & b_2 & 1 & b_4 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} = \mathbf{0}$$

Then,

$$\begin{aligned} b_4 + 1 = 0 &\quad \rightarrow \quad b_4 = 1 \\ b_2 + 1 + 1 = 0 &\quad \rightarrow \quad b_2 = 0 \\ b_1 + 1 + 1 = 0 &\quad \rightarrow \quad b_1 = 0 \end{aligned}$$

Therefore the encoded message is 0011001.

#